P2P Encrypted Payment Terminals
Integrated with the Keystroke Payment Module

The Keystroke Payment Module (KeyPay) provides fast, reliable and secure handling of sensitive payment card data for all current versions of Keystroke POS software. KeyPay is an included component of Keystroke POS software, providing a fully integrated solution for accepting and processing most types of credit, debit and gift cards (including EBT, PIN Debit, and signature capture functionality).

The preferred and most secure method of processing electronic payments through Keystroke POS with KeyPay utilizes P2Pe (point-to-point encryption, also known as end-to-end or E2E) which significantly reduces a merchant’s risk of a data breach while at the same time easing the task of verifying PCI DSS compliance. Configuring the Keystroke POS system for P2Pe requires use of a card swipe device encoded with a unique encryption algorithm that can only be decrypted by the merchant service provider Mercury Payment Systems.

Because the P2Pe device instantly encrypts swiped or manually keyed card data, the POS system never stores, processes, transmits, or has access to raw cardholder data. Keystroke POS transfers the non-sensitive encrypted data from the P2Pe device to KeyPay which sends it on to the merchant services provider where it can be decrypted and processed. Non-sensitive masked card information and tokens are then used by Keystroke and KeyPay to safely display the payment information and provide means for future reference.

Keystroke POS and KeyPay software fully comply with the Payment Card Industry Security Standards Council (PCI) Payment Application Data Security Standards (PA-DSS). Proper use of Keystroke software enables merchants to fully comply with the PCI DSS, but does not in itself guarantee compliance. See PCISecurityStandards.org for more.

Questions?
Consult with an Authorized Keystroke Dealer or call SBS at 800.359.3458 today!